(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2005-136870
(P2005-136870A)
(43)公開日　平成17年5月26日(2005.5.26)

(51)Int.Cl.[7]	F I			チーマコード（参考）
H04L 9/16	H04L	9/00	643	5J104
H04L 9/10	H04L	9/00	621A	

審査請求 未請求　請求項の数 14　OL　（全 12 頁）

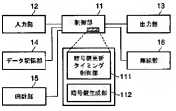
(21)出願番号　特願2003-372991(P2003-372991)
(22)出願日　平成15年10月31日(2003.10.31)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(74)代理人　100058479
弁理士　鈴江　武彦
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100084618
弁理士　村松　貞男
(74)代理人　100092196
弁理士　橋本　良郎

最終頁に続く

(54)【発明の名称】電子機器および暗号鍵更新制御方法

(57)【要約】
【課題】暗号鍵の更新を適切なタイミングで実行可能とした電子機器を提供する。
【解決手段】暗号鍵生成部１１２による暗号鍵の生成・更新が行われた後、暗号鍵更新タイミング制御部１１１は、その時からの経過時間が最短保有時間や最長保有時間に達していないかどうかを監視する。そして、最短保有時間が経過すると、暗号鍵更新タイミング制御部１１１は、無線部１６による無線通信の実行有無を監視し、もし、無線通信が実行されていない状態を検知したら、そのタイミングで暗号鍵の生成・更新を暗号鍵生成部１１２に行わせる。また、この状態を検知できないまま最長保有時間が経過すると、このタイミングで、暗号鍵更新タイミング制御部１１１は、無線通信の一時中断を無線部１６に指示し、その中断中に、暗号鍵の生成・更新を暗号鍵生成部１１２に行わせる。
【選択図】　図２



【特許請求の範囲】
【請求項１】
データ通信手段と、
前記データ通信手段により送信されるデータの暗号化に用いる暗号鍵を生成する暗号鍵生成手段と、
前記データ通信手段によるデータ通信状態を監視する監視手段と、
前記暗号鍵生成手段により暗号鍵が生成されてからの経過時間を算出する時間算出手段と、
前記時間算出手段により算出された経過時間が予め定められた暗号鍵保有時間に達した後、前記監視手段によりデータ通信が実行中ではない状態が検知されたタイミングで前記暗号鍵生成手段に新たな暗号鍵を生成させる暗号鍵更新制御手段と
を具備することを特徴とする電子機器。
【請求項２】
前記暗号鍵更新制御手段は、さらに、前記監視手段によりデータ通信が実行中ではない状態が検知されないまま、前記時間算出手段により算出された時間が予め定められた最長保有時間に達したタイミングで前記暗号鍵生成手段に新たな暗号鍵を生成させる手段を有することを特徴とする請求項１記載の電子機器。
【請求項３】
前記暗号鍵更新制御手段は、最長保有時間に達したタイミングで前記暗号鍵生成手段に新たな暗号鍵を生成させる場合に、前記データ通信手段にデータ通信を中断させる手段を有することを特徴とする請求項２記載の電子機器。
【請求項４】
前記データ通信手段は、IEEE802.11規約に準拠した無線通信を実行し、前記暗号鍵生成手段は、4-way handshake処理を実行して前記暗号鍵を生成することを特徴とする請求項１、２または３記載の電子機器。
【請求項５】
前記最短保有時間および最長保有時間を記憶する記憶手段と、
前記記憶手段に記憶された最短保有時間および最長保有時間を設定する設定手段と
をさらに具備することを特徴とする請求項２または３記載の電子機器。
【請求項６】
データ通信手段と、
前記データ通信手段により送信されるデータの暗号化に用いる暗号鍵を生成する暗号鍵生成手段と、
前記データ通信手段によるデータ通信状態を監視する監視手段と、
前記監視手段によりデータ通信の終了が検知された後、次のデータ通信の開始が検知されない状態の経過時間を算出する第１の時間算出手段と、
前記第１の時間算出手段により算出された経過時間が予め定められた基準間隔時間に達した後、前記監視手段によりデータ通信の開始が検知されたタイミングで前記暗号鍵生成手段に新たな暗号鍵を生成させる暗号鍵更新制御手段と
を具備することを特徴とする電子機器。
【請求項７】
前記暗号鍵生成手段により暗号鍵が生成されてからの経過時間を算出する第２の時間算出手段をさらに具備し、
前記暗号鍵更新制御手段は、さらに、前記監視手段によりデータ通信が実行中である状態が検知された状態で、前記第２の時間算出手段により算出された経過時間が予め定められた暗号鍵保有時間に達したタイミングで前記暗号鍵生成手段に新たな暗号鍵を生成させる手段を有することを特徴とする請求項６記載の電子機器。
【請求項８】
前記暗号鍵更新制御手段は、暗号鍵保有時間に達したタイミングで前記暗号鍵生成手段に新たな暗号鍵を生成させる場合に、前記データ通信手段にデータ通信を中断させる手段

を有することを特徴とする請求項７記載の電子機器。
【請求項９】
前記データ通信手段は、IEEE802.11i規約に準拠した無線通信を実行し、前記暗号鍵生成手段は、4-way handshake処理を実行して前記暗号鍵を生成することを特徴とする請求項６、７または８記載の電子機器。
【請求項１０】
前記基準間隔時間および暗号鍵保有時間を記憶する記憶手段と、
前記記憶手段に記憶された基準間隔時間および暗号鍵保有時間を設定する設定手段とをさらに具備することを特徴とする請求項７または８記載の電子機器。
【請求項１１】
データ通信手段と、前記データ通信手段により送信されるデータの暗号化に用いる暗号鍵を生成する暗号鍵生成手段とを有する電子機器の暗号鍵更新制御方法であって、
前記データ通信手段によるデータ通信状態を監視し、
前記暗号鍵生成手段により暗号鍵が生成されてからの経過時間を算出し、
前記算出した経過時間が予め定められた暗号鍵保有時間に達した後、データ通信が実行中ではない状態を検知したタイミングで前記暗号鍵生成手段に新たな暗号鍵を生成させることを特徴とする暗号鍵更新制御方法。
【請求項１２】
さらに、データ通信が実行中ではない状態を検知しない状態で、前記算出した経過時間が予め定められた最長保有時間に達したタイミングで前記暗号鍵生成手段に新たな暗号鍵を生成させることを特徴とする請求項１１記載の暗号鍵更新制御方法。
【請求項１３】
データ通信手段と、前記データ通信手段により送信されるデータの暗号化に用いる暗号鍵を生成する暗号鍵生成手段とを有する電子機器の暗号鍵更新制御方法であって、
前記データ通信手段によるデータ通信状態を監視し、
データ通信の終了を検知した後、次のデータ通信の開始を検知しない状態の第１の経過時間を算出し、
前記算出した第１の経過時間が予め定められた基準間隔時間に達した後、データ通信の開始を検知したタイミングで前記暗号鍵生成手段に新たな暗号鍵を生成させることを特徴とする暗号鍵更新制御方法。
【請求項１４】
さらに、前記暗号鍵生成手段により暗号鍵が生成されてからの第２の経過時間を算出し、
データ通信が実行中である状態を検知した状態で、前記第２の経過時間が予め定められた暗号鍵保有時間に達したタイミングで前記暗号鍵生成手段に新たな暗号鍵を生成させることを特徴とする請求項１３記載の暗号鍵更新制御方法。
【発明の詳細な説明】
【技術分野】
【０００１】
この発明は、例えばパーソナルコンピュータやアクセスポイントなどの電子機器におけるデータ通信時の暗号化技術に関する。
【背景技術】
【０００２】
近年の無線通信技術の向上に伴い、例えばオフィス環境などでは、ケーブルを敷設して複数の電子機器間を接続するのではなく、無線によって複数の電子機器間を接続する無線ＬＡＮ（Local Area Network）が普及し始めている。この無線ＬＡＮでは、無線通信路を介してデータを送受信するため、データの漏洩を防ぐためのセキュリティ対策として、ＷＥＰ（Wired Equivalent Privacy）などによる暗号化を行うのが一般的である。
【０００３】
ＷＥＰは、固定的な暗号鍵を用いてデータを暗号化する暗号化システムであるが、最近

では、より安全性の高いセキュリティ機能を実現するために、暗号鍵を更新可能としたＴＫＩＰ（Temporal Key Integrity Protocol）、ＷＲＡＰ（Wireless Robust Authenticated Protocol）、ＣＣＭＰ（Counter-Mode/CBC-MAC protocol）といった暗号化システムが注目を集めている。そして、このＴＫＩＰ、ＷＲＡＰ、ＣＣＭＰは、現在策定中であるＷＰＡ（Wi-Fi Protected Access）やIEEE802.11iで採用が予定されており、ＷＰＡやIEEE802.11iでは、これらの暗号化システムで使用される暗号鍵を任意に更新することのできる仕組みが定義されている。

【０００４】

このようなことから、この暗号鍵を適切なタイミングで行うための手法も種々提案されている（例えば特許文献１参照）。この特許文献１の手法では、１日を「朝」、「昼」、「晩」、「夜」などの複数の時間帯に分け、この時間帯毎にデータ通信状態を分析することによって、暗号鍵の更新タイミングを決定する。これにより、暗号鍵の更新処理がデータ通信処理に影響を及ぼしてしまう確率を低下させることができる。

【特許文献１】米国特許第５，７０８，７１１号明細書

【発明の開示】

【発明が解決しようとする課題】

【０００５】

ところで、この特許文献１の手法は、あくまで統計上での推測であり、現実に最適なタイミングで暗号鍵が更新されているかどうかは配慮されていない。例えば無線ＬＡＮはIEEE802.11bで11Mbps、IEEE802.11a,IEEE802.11gでは54Mbpsという高いスループット能力をもつことから、単なるデータ通信だけでなく、リアルタイム性が必要とされるテレビやビデオなどの映像を伝送する手段としても用いられている。そして、このようなリアルタイム性が必要とされるデータでは、その転送中に暗号鍵の更新を行うと、映像や音声が途切れることが予想され、その使い勝手を著しく阻害する。このように、暗号鍵を更新するタイミングの選定は非常に重要である。

【０００６】

この発明は、このような事情を考慮してなされたものであり、暗号鍵の更新を適切なタイミングで実行可能とした電子機器および同機器の暗号鍵更新制御方法を提供することを目的とする。

【課題を解決するための手段】

【０００７】

前述の目的を達成するために、この発明の電子機器は、データ通信手段と、前記データ通信手段により送信されるデータの暗号化に用いる暗号鍵を生成する暗号鍵生成手段と、前記データ通信手段によるデータ通信状態を監視する監視手段と、前記暗号鍵生成手段により暗号鍵が生成されてからの経過時間を算出する時間算出手段と、前記時間算出手段により算出された経過時間が予め定められた暗号鍵保有時間に達した後、前記監視手段によりデータ通信が実行中ではない状態が検知されたタイミングで前記暗号鍵生成手段に新たな暗号鍵を生成させる暗号鍵更新制御手段とを具備することを特徴とする。

【０００８】

また、この発明の電子機器は、前記暗号鍵更新制御手段が、さらに、前記監視手段によりデータ通信が実行中ではない状態が検知されないまま、前記時間算出手段により算出された時間が予め定められた視聴保有時間に達したタイミングで前記暗号鍵生成手段に新たな暗号鍵を生成させる手段を有することを特徴とする。

【０００９】

この発明の電子機器においては、例えばデータ通信が実行されていない、つまり暗号鍵更新に適した状況にあっても、前回の暗号鍵更新時から最短保有時間が経過するまでは、暗号鍵更新を行わないようにすることにより、必要以上に頻繁に暗号鍵更新が発生することを抑止する。また、この最短保有時間が経過した後、データ通信が実行中のまま、つまり暗号鍵更新に不適な状況のまま、前回の暗号鍵更新時から最長保有時間が経過した場合には、安全性を重視し、そのデータ通信を一旦中断して暗号鍵更新を実行する。

【００１０】
このように、この電子機器によれば、効率性と安全性とのバランスを考慮した適切なタイミングでの暗号鍵更新が実行される。
【発明の効果】
【００１１】
この発明によれば、暗号鍵の更新を適切なタイミングで実行可能とした電子機器および同機器の暗号鍵更新制御方法を提供できる。
【発明を実施するための最良の形態】
【００１２】
以下、図面を参照してこの発明の実施形態を説明する。
【００１３】
（第１実施形態）
まず、この発明の第１実施形態について説明する。
【００１４】
図１には、この発明の第１実施形態に係る無線ＬＡＮ通信システムの接続形態が示されている。パーソナルコンピュータ１は、無線通信機能を搭載した例えばノートブックタイプ等の情報処理装置であり、必要に応じて、アクセスポイント２を介してネットワーク３に接続する。ネットワーク３には、他のパーソナルコンピュータなどの様々な情報処理装置が接続されていたり、外部ネットワークがさらに接続されており、パーソナルコンピュータ１は、これらとの間でデータの送受信が可能である。
【００１５】
アクセスポイント２は、パーソナルコンピュータ１とネットワーク３との間を中継する中継装置であり、パーソナルコンピュータ１向けに無線ＬＡＮ４用の無線サービスエリアを形成する一方で、有線ＬＡＮケーブル５によりネットワーク３に収容されている。つまり、パーソナルコンピュータ１とアクセスポイント２とは、無線によりデータを送受信し合う電子機器であり、データを送信する際、そのデータを暗号鍵を使って暗号化する機能を双方が備えている。そして、この第１実施形態の無線ＬＡＮ通信システムは、パーソナルコンピュータ１およびアクセスポイント２が、暗号鍵の更新を適切なタイミングで実行可能とした点を特徴としており、以下、この点について詳述する。なお、ここでは、パーソナルコンピュータ１が主導権をもって暗号鍵の更新を制御するものと想定し、パーソナルコンピュータ１に主眼を置いて説明を行っていく。
【００１６】
図２は、パーソナルコンピュータ１の構成を示す図である。図２に示すように、パーソナルコンピュータ１は、制御部１１、入力部１２、出力部１３、データ記憶部１４、時計部１５および無線部１６の各部を有している。
【００１７】
制御部１１は、このパーソナルコンピュータ１の各種制御を司り、後述する暗号鍵更新タイミング制御部１１１と暗号鍵生成部１１２を有している。入力部１２は、例えばキーボードやマウス等を介して各種情報や操作指示を入力する。一方、出力部１３は、例えばディスプレイやスピーカ等を介して各種情報を出力する。データ記憶部１４は、例えばＥＥＰＲＯＭやＨＤＤ等、各種データを格納するメモリデバイスである。時計部１５は、例えば独自の電源を備えてパーソナルコンピュータ１が使用するシステム時刻を計数する時計モジュールである。そして、無線部１６は、例えばIEEE802.11i規約に準拠した無線通信を実行する。
【００１８】
前述したように、このパーソナルコンピュータ１は、アクセスポイント２との間で無線によりデータを送受信しており、また、自身が主導権をもって送信データを暗号化するための暗号鍵を更新する。暗号鍵更新タイミング制御部１１１は、この暗号鍵の更新タイミングを制御するものであり、一方、暗号鍵生成部１１２は、通信相手であるアクセスポイント２と同期を取りながら暗号鍵を生成・更新するものである。ここで、暗号鍵更新タイ

ミング制御部１１１がどのような原理で暗号鍵の更新タイミングを選定するのかを図３を参照しながら説明する。

【００１９】

暗号鍵生成部１１２による暗号鍵の生成・更新が行われると（図３の（１））、暗号鍵更新タイミング制御部１１１は、その時の時刻を時計部１５から取得する。また、暗号鍵更新タイミング制御部１１１は、データ記憶部１４に記憶された最短保有時間データと最長保有時間データとを事前に取得しており、以降、この暗号鍵の生成・更新時からの経過時間が最短保有時間や最長保有時間に達していないかどうかを監視する。

【００２０】

最短保有時間および最長保有時間は、暗号鍵更新間隔の許容範囲を一組みで定義するものであり、最短保有時間は、必要以上に暗号鍵が更新されるのを防ぐために設けられ、一方、最長保有時間は、安全性を確保するために設けられる。これらは、制御部１１が提供するＧＵＩ等を介してユーザにより設定されてデータ記憶部１４に記憶される。

【００２１】

従って、暗号鍵更新タイミング制御部１１１は、前回の暗号鍵の生成・更新が行われてから最短保有時間が経過するまで（図３の（２））、暗号鍵の生成・更新を暗号鍵生成部１１２に行わせることはない。また、この最短保有時間が経過すると、暗号鍵更新タイミング制御部１１１は、無線部１６による無線通信の実行有無を監視して、もし、無線通信が実行されていない状態を検知したら、そのタイミングで暗号鍵の生成・更新を暗号鍵生成部１１２に行わせる。これにより、暗号鍵の更新処理がデータ通信処理に影響を及ぼすこともない。

【００２２】

また、無線通信が実行されていない状態を検知できないまま、つまり、暗号鍵を生成・更新するタイミングを得られないまま、前回の暗号鍵の生成・更新が行われてからの経過時間が最長保有時間にまで達すると（図３の（３））、このタイミングで、暗号鍵更新タイミング制御部１１１は、無線通信の一時中断を無線部１６に指示し、その中断中に、暗号鍵の生成・更新を暗号鍵生成部１１２に行わせる。これにより、無線によるデータ通信の安全性を確保する。

【００２３】

このように、暗号鍵更新タイミング制御部１１１は、効率性と安全性とのバランスを考慮した適切なタイミングでの暗号鍵更新を実現する。

【００２４】

次に、図４および図５を参照して、このパーソナルコンピュータ１が実行する暗号鍵更新制御の動作手順を説明する。

【００２５】

まず、図４を参照して、パーソナルコンピュータ１がアクセスポイント２との接続・認証を経て最初の暗号鍵生成を行うまでの流れを説明する。

【００２６】

制御部１１は、まず、アクセスポイント２が周囲にあるかどうかを確認するため、スキャン（scan）を実行する（ステップＡ１）。ここで、アクセスポイント２があることが確認できると、制御部１１は、このアクセスポイント２とジョイン（JOIN）を行い、このアクセスポイント２と同期をとる（ステップＡ２）。

【００２７】

同期がとれたら、制御部１１は、続いて認証（authentication）を実行する（ステップＡ３）。ここでのauthenticationは、オープンシステム認証と呼ばれ、特別な認証処理はせずに、パーソナルコンピュータ１から認証要求を行うと、アクセスポイント２はそのまま認証要求を受け入れる。

【００２８】

次に、制御部１１は、アクセスポイント２との接続処理（assosiation）を行う（ステップＡ４）。そして、この接続が完了すると、暗号鍵生成部１１２が、4-way handshake

と呼ばれる暗号鍵の生成をアクセスポイント２と共に実行する（ステップＡ５）。

【００２９】

図５は、パーソナルコンピュータ１が行う暗号鍵の更新タイミング制御の流れを示すフローチャートである。

【００３０】

前述の4-way handshakeによる暗号鍵の生成を暗号鍵生成部１１２に行わせると（ステップＢ１）、暗号鍵更新タイミング制御部１１１は、時計部１５からシステム時刻を取得して記憶する（ステップＢ２）。そして、暗号鍵更新タイミング制御部１１１は、無線部１６に対して暗号データ通信の許可を指示し（ステップＢ３）、この無線部１６による無線通信の実行有無の監視を開始する（ステップＢ４）。

【００３１】

もし、データ通信が実行されていなければ（ステップＢ４のＮＯ）、暗号鍵更新タイミング制御部１１１は、暗号鍵更新間隔の最短保有時間が経過したかどうかを調べ（ステップＢ５）、最短保有時間を経過していないならば（ステップＢ５のＮＯ）、ステップＢ４のデータ通信有無のチェックに戻る。一方、このデータ通信の未実行時に最短保有時間を経過していたら（ステップＢ５のＹＥＳ）、その時点で、暗号鍵更新タイミング制御部１１１は、無線部１６に対して暗号データ通信の不許可を指示し（ステップＢ６）、暗号データ通信を停止させてから、ステップＢ１に戻って、4-way handshakeによる暗号鍵の生成を暗号鍵生成部１１２に行わせる。

【００３２】

また、データ通信が実行されていた場合には（ステップＢ４のＹＥＳ）、暗号鍵更新タイミング制御部１１１は、暗号鍵更新間隔の最長保有時間が経過したかどうかを調べ（ステップＢ７）、最長保有時間を経過していないならば、（ステップＢ７のＮＯ）、ステップＢ４のデータ通信有無のチェックに戻る。一方、このデータ通信の実行時に最長保有時間を経過していたら（ステップＢ７のＹＥＳ）、その時点で、暗号鍵更新タイミング制御部１１１は、無線部１６に対して暗号データ通信の不許可を指示し（ステップＢ６）、暗号データ通信を停止させてから、ステップＢ１に戻って、4-way handshakeによる暗号鍵の生成を暗号鍵生成部１１２に行わせる。

【００３３】

以上のような制御を行うことにより、データ通信中における暗号鍵の更新を低減することができ、かつ、必要な安全性を維持することができる。また、最短保有時間を設定することにより、データ通信のない時に、無意味に暗号鍵の更新を行わないようにすることができる。

【００３４】

（第２実施形態）

次に、この発明の第２実施形態について説明する。

【００３５】

前述した第１実施形態の無線ＬＡＮ通信システムでは、暗号鍵更新の主導権をもったパーソナルコンピュータ１が、最短保有時間および最長保有時間をもとに、暗号鍵の更新タイミングを制御した。これに対して、この第２実施形態の無線ＬＡＮシステムでは、最短保有時間に代えて、暗号データ通信が所定の時間以上途絶えたか否かを判定するための基準間隔時間を利用して、暗号鍵の更新タイミングを制御する。この無線ＬＡＮ通信システムでは、基準間隔時間を越えた後に発生した暗号データ通信は、新たなデータ通信であると判定し、そのデータ通信の開始時に、暗号鍵の更新を行うようにする。この基準間隔時間も、制御部１１が提供するＧＵＩ等を介してユーザにより設定されてデータ記憶部１４に記憶されるデータであり、暗号鍵更新タイミング制御部１１１は、起動時等に当該データを取得する。

【００３６】

図６は、この第２実施形態における暗号鍵更新タイミング制御部１１１の暗号鍵更新タイミング選定原理を説明するための図である。

【００３７】
ここでは、ある暗号データ通信が終了した後、長時間を渡って暗号データ通信が途絶える場合を想定する。この場合、第１実施形態の場合、図６（Ａ）に示すように、最短保有時間が経過する度に（図６（Ａ）の（２），（２）’，（２）”…）、暗号鍵生成部１１２による暗号鍵の生成・更新が繰り返されることになる。これらの暗号鍵は、暗号データ通信に一度も使用されていないので、盗難されているおそれがなく、無意味に暗号鍵の更新を行っているともいえる。
【００３８】
そこで、この第２実施形態では、ある暗号データ通信が終了した後、暗号データ通信が途絶えた状態が基準間隔時間を越えたら（図６（Ｂ）の（２））、次の暗号データ通信の開始を監視し、暗号データ通信の開始を検知したら（図６（Ｂ）の（３））、このタイミングで、暗号鍵の生成・更新を暗号鍵生成部１１２に行わせる。
【００３９】
つまり、この第２実施形態では、図６（Ａ）の（２），（２）’，（２）”のような無意味な暗号鍵の更新を排除する。また、新たな暗号データ通信の開始時に、暗号鍵の更新を行うようにすることにより、第１実施形態では偶然により起こり得る、新たな暗号データ通信を開始した直後に、最短保有時間が訪れ、その状態のまま最長保有時間に達してしまった場合のような、つまり、例えば図６（Ａ）の（１）に示したような暗号データ通信中の暗号鍵更新を低減する。
【００４０】
図７は、第２実施形態のパーソナルコンピュータ１が行う暗号鍵の更新タイミング制御の流れを示すフローチャートである。
【００４１】
暗号鍵の生成を暗号鍵生成部１１２に行わせると（ステップＣ１）、暗号鍵更新タイミング制御部１１１は、時計部１５からシステム時刻（時間Ｂ）を取得して記憶する（ステップＣ２）。ここでの時間Ｂの取得は、データ通信が途絶えている時間を算出するための開始点のクリアである。また、このとき、暗号鍵更新タイミング制御部１１１は、この取得したシステム時間を、暗号鍵を生成した時間（時間Ａ）としても記憶しておく（ステップＣ３）。そして、暗号鍵更新タイミング制御部１１１は、無線部１６に対して暗号データ通信の許可を指示し（ステップＣ４）、この無線部１６による無線通信の実行有無の監視を開始する（ステップＣ５）。
【００４２】
もし、データ通信が実行されていなければ（ステップＣ５のＮＯ）、暗号鍵更新タイミング制御部１１１は、時間Ｂ、つまり最後のデータ通信時からの経過時間が基準間隔時間を経過したかどうかを調べ（ステップＣ６）、基準間隔時間を経過していないならば（ステップＣ６のＮＯ）、ステップＣ５のデータ通信有無のチェックに戻る。一方、この基準間隔時間を経過していたら（ステップＣ６のＹＥＳ）、暗号鍵更新タイミング制御部１１１は、今度は、無線部１６による無線通信が開始されたかどうかを検知するために、無線部１６による無線通信の実行有無の監視を開始する（ステップＣ７）。そして、無線部１６による無線通信が開始されたら（ステップＣ７のＹＥＳ）、その時点で、暗号鍵更新タイミング制御部１１１は、無線部１６に対して暗号データ通信の不許可を指示し（ステップＣ８）、暗号データ通信を停止させてから、ステップＣ１に戻って、4-way handshakeによる暗号鍵の生成を暗号鍵生成部１１２に行わせる。なお、この場合、データ通信開始前にデータ通信を停止させるため、データ通信の開始が遅れるが、データの途切れは起こらない。
【００４３】
また、データ通信が実行されていた場合には（ステップＣ５のＹＥＳ）、暗号鍵更新タイミング制御部１１１は、まず、時計部１５からシステム時刻（時間Ｂ）を取得して記憶し直す（ステップＣ９）。そして、暗号鍵更新タイミング制御部１１１は、暗号鍵更新間隔の最長保有時間が経過したかどうかを調べ（ステップＣ１０）、最長保有時間を経過し

ていないならば、（ステップＣ１０のＮＯ）、ステップＣ５のデータ通信有無のチェックに戻る。一方、このデータ通信の実行時に最長保有時間を経過していたら（ステップＣ９のＹＥＳ）、その時点で、暗号鍵更新タイミング制御部１１１は、無線部１６に対して暗号データ通信の不許可を指示し（ステップＣ８）、暗号データ通信を停止させてから、ステップＣ１に戻って、4-way handshakeによる暗号鍵の生成を暗号鍵生成部１１２に行わせる。

【００４４】

以上のような制御を行うことにより、データ通信を開始してからの連続通信時間が、そのまま暗号鍵の最大更新間隔となるため、安全性を維持しつつ、データ通信中における暗号鍵の更新を実行する可能性をさらに低減することができる。

【００４５】

なお、本発明は上記実施形態そのままに限定されるものではなく、実施段階ではその要旨を逸脱しない範囲で構成要素を変形して具体化できる。例えば、上記実施形態をアクセスポイント内に配置しても実現可能である。また、上記実施形態に開示されている複数の構成要素の適宜な組み合わせにより、種々の発明を形成できる。例えば、実施形態に示される全構成要素から幾つかの構成要素を削除してもよい。さらに、異なる実施形態にわたる構成要素を適宜組み合わせてもよい。

【図面の簡単な説明】

【００４６】

【図１】本発明の第１実施形態に係る無線ＬＡＮ通信システムの接続形態を示す図

【図２】同第１実施形態のパーソナルコンピュータの構成を示す図

【図３】同第１実施形態における暗号鍵更新タイミング制御部の暗号鍵更新タイミング選定原理を説明するための図

【図４】同第１実施形態のパーソナルコンピュータがアクセスポイントとの接続・認証を経て最初の暗号鍵生成を行うまでの流れを示すフローチャート

【図５】同第１実施形態のパーソナルコンピュータが行う暗号鍵の更新タイミング制御の流れを示すフローチャート

【図６】同第２実施形態における暗号鍵更新タイミング制御部の暗号鍵更新タイミング選定原理を説明するための図

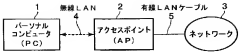
【図７】同第１実施形態のパーソナルコンピュータが行う暗号鍵の更新タイミング制御の流れを示すフローチャート

【符号の説明】

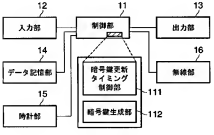
【００４７】

１…パーソナルコンピュータ、２…アクセスポイント、３…ネットワーク、４…無線ＬＡＮ、５…有線ＬＡＮケーブル、１１…制御部、１２…入力部、１３…出力部、１４…データ記憶部、１５…時計部、１６…無線部、１１１…暗号鍵更新タイミング制御部、１１２…暗号鍵生成部。

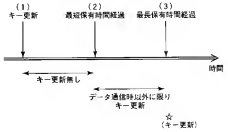
【図１】



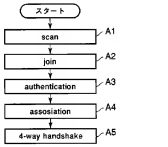
【図２】



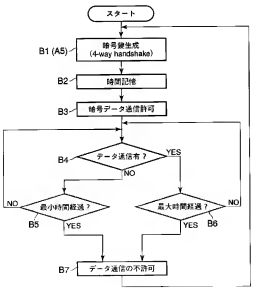
【図３】



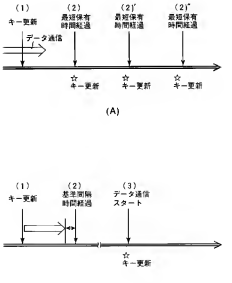
【図４】



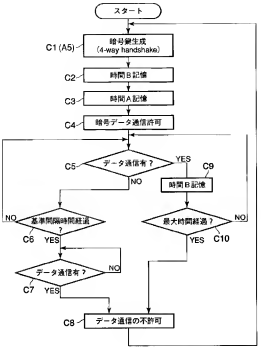
【図５】



【図６】



【図７】


スタート
C1 (A5)
暗号鍵生成
(4-way handshake)
C2
時間B記憶
C3
時間A記憶
C4
暗号データ通信許可
C5
データ通信有？
YES
NO
C9
時間B記憶
NO
基準間隔時間経過
YES
C6
最大時間経過？
NO
YES
C10
データ通信有？
NO
YES
C7
C8
データ通信の不許可

フロントページの続き

(72)発明者 相原 督弘
東京都青梅市末広町２丁目９番地 株式会社東芝青梅事業所内
Ｆターム(参考) 5J104 AA16 AA34 EA04 EA18 JA03 NA02 PA01